

## **REMARKS**

### **I. Introduction**

Claims 10-11 and 14-18 are pending in the present application. Claim 10 has been amended. In view of the following explanations, it is respectfully submitted that all of the presently pending claims 10-11 and 14-18 are allowable, and reconsideration of the pending claims is respectfully requested.

### **II. Rejection of Claims 10, 11 & 14-18**

Claims 10, 11 and 14-18 were rejected under 35 U.S.C. § 103(a) as being obvious in view of the combination of U.S. Patent 5,745,576 ("Abraham") and U.S. Patent 4,797,672 ("Kousa"). Applicants respectfully submit that this rejection should be withdrawn for the following reasons.

In rejecting a claim under 35 U.S.C. § 103(a), the Office bears the initial burden of presenting a prima facie case of obviousness. In re Rijckaert, 9 F.3d 1531, 1532, 28 U.S.P.Q.2d 1955, 1956 (Fed. Cir. 1993). To establish prima facie obviousness, three criteria must be satisfied. First, there must be some suggestion or motivation to modify or combine the reference teachings. In re Fine, 837 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988). The prior art must suggest combining the features in the manner contemplated by the claim. See Northern Telecom, Inc. v. Datapoint Corp., 908 F.2d 931, 934 (Fed. Cir. 1990), cert. denied, 111 S. Ct. 296; In re Bond, 910 F.2d 831, 834 (Fed. Cir. 1990). This teaching or suggestion to make the claimed combination must be found in the prior art and not based on the application disclosure. In re Vaeck, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991). Second, there must be a reasonable expectation of success. In re Merck & Co., Inc., 800 F.2d 1091, 231 U.S.P.Q. 375 (Fed. Cir. 1986). Third, the prior art reference(s) must teach or suggest all of the claim features. In re Royka, 490 F.2d 981, 180 U.S.P.Q. 580 (C.C.P.A. 1974). To the extent that the Examiner may be relying on the doctrine of inherent disclosure for the anticipation rejection, the Examiner must provide a "basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristics necessarily flow from the teachings of the applied art." (See M.P.E.P. § 2112; emphasis in original; see also Ex parte Levy, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990)).

Claim 10 recites the following:

10. **A system for access authorization**, comprising:

a base device including a computer, wherein the base device initially transmits a prompt signal within a framework of an initial prompt/reply cycle that is successfully carried out, **and wherein the prompt signal is stored in the base device**; and

at least one remote control storing the initially transmitted prompt signal from the initial prompt/reply cycle;

wherein, in an access authorization process, **subsequent to the previous, initial prompt/reply cycle that is successfully carried out**, the at least one remote control transmits to the base device a code word containing a reply, the reply being formed at least partially as a function of the prompt signal stored in the at least one remote control, wherein the base device receives the code word containing the reply and compares the reply contained in the code word with a required reply, wherein an access is authorized if the reply contained in the code word agrees with the required reply, **and wherein the prompt signal stored in the base device is erased when a number of failed agreements of the reply and the required reply exceeds a specifiable limiting value.**

In the Examiner's Answer, the Examiner contended that "[w]ith regard to applicant's argument that Abraham does not teach a system for access authorization, . . . this has never been claimed," since the "claims state 'a system for controlling an access authorization.'" In response, Applicants have amended claim 10 to explicitly recite a "system for access authorization." Abraham clearly does not teach or suggest **a system for access authorization**, as recited in the present claims; instead, Abraham only discusses the initialization procedure of a cryptographic terminal in a cryptographic system (column 5, lines 10 through 12 and 25 through 26: The initial key, or a key derived from it, is used only for **initialization purposes and not for system operation**). Therefore, one skilled in the art would not be motivated by the teachings of Abraham, in combination with the teachings of Kousa, to arrive at the presently claimed subject matter.

Independent of the above, to the extent the Examiner maintains that “the encrypted challenge message must be stored to be decrypted,” the Examiner has yet to provide any supporting document in the examination proceeding, which the Examiner must do in order to support a contention based on Examiner’s personal knowledge. To the extent that the Examiner is contending that feature is inherently disclosed by Abraham, the Examiner must provide a “basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristics necessarily flow from the teachings of the applied art,” which the Examiner has clearly failed to do.

Even if one assumed for the sake of argument that there were some motivation to combine the teachings of Abraham and Kousa, with which assumption Applicants do not agree, the asserted combination still would not teach or suggest to store a prompt from “an initial prompt/reply cycle that is successfully carried out,” and subsequently use the stored prompt. While Kousa discusses, e.g., in column 2, lines 3-10, that two consecutive inquiry/response dialogues (hand shakes) are carried out for system identification in a secure transmission system, nothing in Kousa suggests that the inquiry signal is stored in the node. To the extent the Examiner cites Merritt (U.S. Patent 5,475,756) in support of the proposition that “key exchange to begin a session is well known in the art,” (4/14/06 Advisory Action), Applicants submit that this contention simply does not support the obviousness conclusion because even if “key exchange to begin a session is well known in the art,” as allegedly disclosed by Merritt, it does not logically follow that one of ordinary skill in the art would be motivated to store a prompt from “an initial prompt/reply cycle that is successfully carried out,” and subsequently use the stored prompt. Nothing in Merritt, including col. 6, l. 54-63 (cited by the Examiner in the Advisory Action of April 14, 2006), teaches or suggests exchange of keys or storing a prompt from “an initial prompt/reply cycle that is successfully carried out,” and subsequently use the stored prompt. In fact, Merritt merely indicates that when “a new terminal, such as the ATM 10, is brought on-line . . . , the bank 1 assigns . . . an encryption key K,” and the encryption key is stored “both in the ATM’s storage means 20 and in the bank’s host 2.” (Col. 1, l. 50-63). In another section of Merritt, it is indicated that “the host has an encryption key K1, and the ATM has an encryption key K2,” and “the two keys, K1 and K2, are identical . . . to the key K.” (Col. 5, l. 13-17). Accordingly, it is clear that the encryption keys are simply assigned to the authorized device (e.g., ATM) by the network operator (e.g., the bank), and there is no suggestion of storing a prompt from “an

initial prompt/reply cycle that is successfully carried out,” and subsequently using the stored prompt.

With respect to the Examiner’s assertions that See teaches “terminating a session with a user after a predetermined number of failed login attempts,” and that Schneier teaches “session keys are erased when a session is ended,” and therefore the combination of the teachings of See and Schneier would suggest the claimed feature that “the **prompt signal** stored in the base device **is erased when a number of failed agreements** of the reply and the required reply **exceeds a specifiable limiting value**,” Applicants respectfully note that the overall teachings of the applied references do not support the Examiner’s conclusion. Initially, there is no apparent motivation in the overall teachings of See and Schneier to modify the teachings of one with the other, particularly since each reference is completely silent on the subject taught by the other reference, i.e., See does not suggest anything relating to erasing of session keys, and Schneier doesn’t suggest anything relating to the relevance of predetermined number of failed login attempts. More fundamentally, neither See nor Schneier suggests any **deletion as a function of a number of incorrect attempts**. Accordingly, there is no apparent motivation that one of ordinary skill in the art would selectively combine specific teachings of See and Schneier as asserted by the Examiner in an attempt to arrive at the claimed feature that “the **prompt signal** stored in the base device **is erased when a number of failed agreements** of the reply and the required reply **exceeds a specifiable limiting value**.”

Accordingly, the combination of applied references fails to teach or suggest “in an access authorization process, subsequent to the previous, initial prompt/reply cycle that is successfully carried out, the at least one remote control transmits to the base device a code word containing a reply, the reply being formed at least partially as a function of the prompt signal stored in the at least one remote control,” as recited in claim 10.

Accordingly, for at least the foregoing reasons, claim 10 and its dependent claims 11 and 14-18 are not rendered obvious by the combination of the applied references.

**CONCLUSION**

Applicants respectfully submit that all pending claims of the present application are now in condition for allowance. Prompt reconsideration and allowance of the present application are therefore earnestly solicited.

Respectfully submitted,

 (R.No. 36,197)

Dated: February 13, 2007

By: SONG LEE for Gerard Messina  
Gerard A. Messina  
Reg. No. 35,952

KENYON & KENYON LLP  
One Broadway  
New York, New York 10004  
(212) 425-7200

**CUSTOMER NO. 26646**